操作の両立不可能性と情報擾乱の関係 (量子システム推定の数理)

AUTHOR(S):

濱村, 一航

CITATION:

濱村, 一航. 操作の両立不可能性と情報擾乱の関係 (量子システム推定の数理). 数理解析研究所講究録 2017, 2059: 113-129

ISSUE DATE:

2017-10

URL:

http://hdl.handle.net/2433/237217

数理解析研究所講究録
第2059巻 2017年 113-129

操作の両立不可能性と情報擾乱の関係

京都大学大学院 工学研究科 原子核工学専攻　濵村 一航 †
Ikko Hamamura
Department of Nuclear Engeneering, Kyoto University

概要

量子論において実現可能な操作には様々な制約がある．例えば，量子状態は複製や配送が出来ないという複製 (配送) 禁止定理や，物理量の測定によって情報を取得すると擾乱が起こるという情報と擾乱の関係，位置と運動量のように非可換でシャープな物理量は同時に測定出来ないという一種の不確定性関係はよく知られた操作の制約である．これらの例は，全て本稿で扱う量子論の両立不可能性の一例である．さらに，両立不可能性の一例として紹介した情報と擾乱の関係に関して，状態識別能力が高い測定は擾乱が大きいということを，操作的に前順序関係を導入して定性的に示すと同時に状態識別能力と擾乱の関係を定量化して得た不等式を紹介する．

1　はじめに

1.1　本稿の目的

量子論には，不確定性関係がある[1]．量子論では情報のコピーは出来ない．量子論では，状態から情報を取り出すと，状態は変化してしまう．これらの性質は量子論を特徴づける重要な性質であると同時に，量子情報で量子論が応用される際にも鍵となる役割を果たしている．こういった制約は実験技術からくる制約とは異なり，理論的に不可能な操作があるということを表している．技術的な制約は技術が進歩することにより破れることがあるが，理論的な制約はその理論が正しい限り破られることがない．

測定や情報のコピーは，ある種の操作である．不確定性関係やコピーが出来ないといった性質は，量子論における可能な操作に何かしらの制約があるものと考えられる．先の例の

〒615-8540 京都市西京区京都大学桂
† hamamura@nucleng.kyoto-u.ac.jp

[1] 不確定性関係には様々な種類があるが，本稿で扱うのは同時測定の不確定性関係と呼ばれるものである．有名な例としては，位置と運動量は同時測定出来ないというものがある．また最も有名な量子ゆらぎを用いたRobertson と Kennard の不確定性関係は，状態準備の不確定性であり今回扱うものとは異なる．

ような複数の操作を同時に行なうことは出来ないという制約のことを量子論における操作の両立不可能性 (incompatibility) という．本稿では，この操作の両立不可能性についてレビューを行ない，その操作の両立不可能性の一種である情報と擾乱の関係に関する構造的な議論を行なう．両立不可能性については，[1] にさらに詳しいレビューがある．

本稿は，1 章で基本的な定義を導入し，2 章で操作の両立不可能性を議論する．3 章から 5 章は定性的な情報と擾乱の関係について，状態識別能力と擾乱の関係を用いた定式化 [2] について述べる．6 章ではまとめと今後の展望について述べる．

1.2 状態空間

1.1 でも登場した状態とは物理的な実験状況のことであり，実験系において測定対象をどういった方法で準備するかに依存したものである．ただし，異なる準備方法であったとしても，任意の測定に対して同じ確率分布で測定結果を返す状態は同じ状態とみなしている．

この状態の集合のことを，状態空間という．数学的には状態空間は空でないコンパクト凸集合である．この凸集合であるという性質は状態の確率混合という操作に由来している[2]．すなわち，状態空間を S とすると，確率 p で状態 $s_1 \in S$，確率 $1-p$ で状態 $s_2 \in S$ で混合をした，

$$s = ps_1 + (1-p)s_2 \tag{1}$$

という状態 s も再び状態空間の元であるということを表している．本稿では，簡単のため状態空間は有限次元の実ユークリッド空間 $\mathbb{R}^n$ に埋め込めるものとする．

状態は純粋状態と混合状態との二種類に分類される．純粋状態は状態空間の端点であり，混合状態は純粋状態以外の状態である．状態 s が状態空間 S の端点であるとは，$0 < p < 1$ なる p を用いた凸分解

$$s = ps_1 + (1-p)s_2 \tag{2}$$

が，自明な場合 $(s = s_1 = s_2)$ のみであるときをいう．

Krein-Milman の定理によると，任意の混合状態は純粋状態を確率混合することにより準備できることがわかる．さらに，Carathéodory の定理から，$\mathbb{R}^n$ の凸部分集合の点は高々 $n+1$ 個の純粋状態の確率混合で準備することができる．

状態空間の中で重要なものが二種類ある．1 つは古典論の状態空間で，もう 1 つは量子論の状態空間である．次ではそれぞれの状態空間について述べたい．

---

[2] 本来は状態に和やスカラー倍といったベクトル空間の構造が入っていることは非自明であり，そういった構造を入れず凸構造から議論を始めることもあるが，本稿では凸構造の議論は省略し，状態空間は凸集合であるというところから始めることにする．

1.3 古典論の状態空間

古典論の状態空間は単体である．標準単体は，

$$S_{\mathrm{cl}} = \left\{ (p_0, \ldots, p_{n-1}) \in \mathbb{R}^n \,\middle|\, \sum_{i=0}^{n-1} p_i = 1, p_i \geq 0 \right\} \tag{3}$$

である．状態 $s = (p_0, \ldots, p_{n-1})$ は i 番目の成分が 1 でその他の成分が 0 の純粋状態 $\hat{e}_i$ を確率 p_i で準備して混合した

$$s = \sum_{i=0}^{n-1} p_i \hat{e}_i \tag{4}$$

である．任意の混合状態は純粋状態の確率混合に分解することが出来るが，この端点分解が一意であるという性質が古典論特有の性質である．あとで見るように量子論の混合状態の端点分解は一意ではない．古典論の状態空間は有限個 (n 個) の測定出力の確率分布の集合とみなすことができる．単体の定義に p_i が非負であることがあるが，これは確率が正であることに由来する．$\sum_{i=0}^{n-1} p_i = 1$ は確率の規格化条件とみなすことができる．無限次元の単体を考えることもあるが，本稿の状態空間は有限次元空間に埋め込めるものに限定するのでここでは扱わない．

古典論の状態空間のうち，特に $n = 2$ の物理系を (古典) ビット系という．ビット系の純粋状態は例えば現代のコンピュータや通信の情報処理の資源として用いられている．ビット系の 2 つの純粋状態のうち片方を 0，もう片方を 1 と呼ぶこともある．

1.4 量子論の状態空間

量子論の状態空間は

$$\mathcal{S}(\mathcal{H}) = \{ \rho \in \mathcal{T}(\mathcal{H}) \,|\, \rho \geq 0, \mathrm{tr}\,[\rho] = 1 \} \tag{5}$$

である．ここで，$\mathcal{H}$ はヒルベルト空間，$\mathcal{T}(\mathcal{H})$ はヒルベルト空間 $\mathcal{H}$ に作用するトレース級作用素全体の集合であるとする．本稿で扱う有限次元ヒルベルト空間 $\mathcal{H}$ の場合は $\mathcal{T}(\mathcal{H})$ は $\mathcal{H}$ 上の行列の集合と一致する．量子論における純粋状態は何かしらの単位ベクトル $|\psi\rangle$ を用いて，$|\psi\rangle\langle\psi|$ の形に書けるので，ケットベクトル $|\psi\rangle$ を純粋状態と呼ぶこともある．ここで，ディラックのブラケット記法[3]を用いた．最も単純な量子論の状態空間は $\mathcal{H} = \mathbb{C}^2$ の場合で，この物理系を量子ビット系という．純粋状態 $|0\rangle = (1,0)^{\mathrm{T}}$，$|1\rangle = (0,1)^{\mathrm{T}}$ は，古典ビットの

[3] $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ とする．$\langle\psi|\phi\rangle$ は $|\psi\rangle$ と $|\phi\rangle$ の内積を表す．$|\psi\rangle\langle\psi|$ は $\mathcal{H} \to \mathcal{H}$ なる作用素で，$|\psi\rangle\langle\psi|\,|\phi\rangle := \langle\psi|\phi\rangle|\phi\rangle$ と定義される．

純粋状態 0 と 1 に対応しており，量子情報では計算基底と呼ばれる．トレースが 0 であるパウリ行列，

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{6}$$

を用いると，任意の量子ビット系の状態は

$$\rho = \frac{1}{2}(\mathbf{1} + x\sigma_x + y\sigma_y + z\sigma_z) \tag{7}$$

と書ける．ここで，x, y, z は $x^2 + y^2 + z^2 \leq 0$ を満たす実数である．逆に，この行列 ρ は量子ビット系の状態になっている．したがって，量子ビット系の状態は三次元の単位球と同一視できる．この球のことを Bloch 球という．Bloch 球の中心 $\frac{1}{2}$ を完全混合状態という．$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$，$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ とする．$|0\rangle$ と $|1\rangle$ をそれぞれ確率 $\frac{1}{2}$ で準備しても，$|+\rangle$ と $|-\rangle$ をそれぞれ確率 $\frac{1}{2}$ で準備しても，

$$\frac{\mathbf{1}}{2} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| \tag{8}$$

状態としては同じ完全混合状態を準備することが出来る．したがって，量子論の状態は端点分解が一意であるとは限らない．

1.5 合成系の状態空間

1 ビットだけでは純粋状態は 0 と 1 の二種類しかなく，複雑な情報処理を行なうためには複数のビットが必要である．量子ビットでも同様で，複数の量子ビットを用いた方がより高度な情報処理を行なうことが出来る．そのため，複数の系からなる合成系を考える必要がある．そこでまず，2 つの系からなる合成系を考えたい．瞬間伝送禁止則と局所識別性 [3] から合成系の状態空間はコンパクト凸集合のテンソル積である．コンパクト凸集合のテンソル積は一意に定まらないので [4]，一般には合成系の状態空間は一意に定めることが出来ないが，少なくとも片方の系が古典の場合はそれぞれの系の状態の積状態の (閉) 凸包に一致する [4]．作り方から明らかなように合成系の状態空間は再びコンパクト凸集合になっている．すなわち，状態空間 S_1 か S_2 の少なくとも片方の系が古典であるとすると，S_1 と S_2 の合成系の状態空間 $S_1 \otimes S_2$ は

$$S_1 \otimes S_2 = S_1 \otimes_{\min} S_2 := \overline{\mathrm{Conv}}\{\, s_1 \otimes s_2 \mid s_1 \in S_1, s_2 \in S_2 \,\} \tag{9}$$

である．例えば，古典論の状態は確率分布であるが，古典論の合成系の状態は同時確率分布である．量子論の状態空間 $\mathcal{S}(\mathcal{H}_1)$，$\mathcal{S}(\mathcal{H}_2)$ の合成系 $\mathcal{S}(\mathcal{H}_1) \otimes \mathcal{S}(\mathcal{H}_2)$ はヒルベルト空間のテンソル積で与えられ，

$$\mathcal{S}(\mathcal{H}_1) \otimes \mathcal{S}(\mathcal{H}_2) = \mathcal{S}(\mathcal{H}_1) \otimes_{\mathrm{Q}} \mathcal{S}(\mathcal{H}_2) := \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2) \tag{10}$$

である．量子論の合成系の構造については，[5] で詳しく議論している．少なくとも片方が古典論の場合の式 (9) で与えられる定義をそのまま量子論に当てはめて最小テンソル積状態空間 $\mathcal{S}(\mathcal{H}_1) \otimes_{\min} \mathcal{S}(\mathcal{H}_2)$ を考える．このとき，

$$\mathcal{S}(\mathcal{H}_1) \otimes_{\min} \mathcal{S}(\mathcal{H}_2) \subset \mathcal{S}(\mathcal{H}_1) \otimes_{\mathrm{Q}} \mathcal{S}(\mathcal{H}_2) \tag{11}$$

が成り立つ．この $\mathcal{S}(\mathcal{H}_1) \otimes_{\min} \mathcal{S}(\mathcal{H}_2)$ の元はセパラブル状態と呼ばれ，局所操作と古典通信 (LOCC) で準備可能な状態として知られている．セパラブル状態ではない量子状態，すなわち $\mathcal{S}(\mathcal{H}_1) \otimes_{\mathrm{Q}} \mathcal{S}(\mathcal{H}_2) \setminus \mathcal{S}(\mathcal{H}_1) \otimes_{\min} \mathcal{S}(\mathcal{H}_2)$ の元のことをエンタングルした状態という．

以上のように，古典論の状態空間と古典論の状態空間，古典論の状態空間と量子論の状態空間のような少なくとも片方が古典の場合と，量子論の状態空間と量子論の状態空間の場合については，合成系の状態空間は定義されている．これ以降の章で出てくる合成系の状態空間はこれら 3 種類である．

1.6 状態変化

準備した状態をそのままにしておくだけでなく，何かしらの操作を行なって状態を変化させることで，計算や通信といった情報処理を行なう．この状態変化について考えたい．状態変化とは状態空間から状態空間への写像である．情報理論で，通信の経路のことをチャンネルということに由来し，状態変化のことをチャンネルということもある．さらにこの写像はアフィンである，すなわち，チャンネル $f\colon S_{\mathrm{in}} \to S_{\mathrm{out}}$ は，$f(s) = f(ps_1 + (1-p)s_2) = pf(s_1) + (1-p)f(s_2)$ という性質を満たす．これは，確率 p で状態 s_1 と確率 $1-p$ で状態 s_2 を準備して混合した状態 $ps_1 + (1-p)s_2$ を状態変化させた状態と，状態 s_1 と状態 s_2 をそれぞれ状態変化させてから確率 p と $1-p$ の割合で混合した状態が同じであるという操作的な要請である．

任意のアフィン写像が実現可能であるとは限らない．特に，量子論の場合はアフィンだけでは不十分である．アフィン写像 $f\colon \mathcal{S}(\mathcal{H}_{\mathrm{in}}) \to \mathcal{S}(\mathcal{H}_{\mathrm{out}})$ と恒等写像 $\mathrm{id}\colon \mathcal{S}(\mathbb{C}^n) \to \mathcal{S}(\mathbb{C}^n)$ を考える．合成系 $\mathcal{S}(\mathcal{H}_{\mathrm{in}} \otimes \mathbb{C}^n)$ について，左側の系に f という状態変化を行ない，右側の系では何も操作しないという恒等操作を行なうことを考える．すなわち，$f \otimes \mathrm{id}$ という写像も物理的に可能な状態変化であってほしい．したがって，この写像 $f \otimes \mathrm{id}$ の終域は合成系 $\mathcal{S}(\mathcal{H}_{\mathrm{out}} \otimes \mathbb{C}^n)$ であるべきだが，実は f がアフィン写像であるというだけでは，$f \otimes \mathrm{id}$ の終域が $\mathcal{S}(\mathcal{H}_{\mathrm{out}} \otimes \mathbb{C}^n)$ より大きくなってしまう場合がある．そこで，任意の正の整数 n について $f \otimes \mathrm{id}$ の終域が $\mathcal{S}(\mathcal{H}_{\mathrm{out}} \otimes \mathbb{C}^n)$ であるということを写像 f に要請する．この条件は f を線型拡張した写像が完全正値トレース保存線型写像 (CPTP 線型写像) であることに他ならない．CPTP 線型写像のことを量子チャンネルということもある．

状態を準備し物理量の測定を行なうと，何かしらの測定出力が得られる．この操作を繰り返すと理想的には確率分布を得ることが出来る．物理量の測定という操作は状態空間から確

率分布への写像とみなすことが出来る．有限個の測定出力をもった確率分布は古典論の状態空間なので，物理量の測定は古典論の状態空間への状態変化である．物理量の測定を表す写像を $\mathsf{M}\colon S \to S_{\mathrm{cl}}$ とする．古典論の状態は $(p_0, \ldots, p_{n-1})$ のように表せ，この成分のラベルが測定出力に対応する．すなわち，1 回 1 回の測定において p_i は i 番目の測定出力が得られる確率と解釈する．各成分の射影を π_i として，$\mathsf{M}_i = \pi_i \circ \mathsf{M}$ と定義する．この写像 $\mathsf{M}_i\colon S \to [0,1]$ をエフェクトという．エフェクトもまたアフィン写像となっている．任意の状態に対して 0 を返すエフェクトをゼロエフェクト，任意の状態に対して 1 を返すエフェクトを単位エフェクトという．

量子論における物理量の測定について述べる．$e\colon \mathcal{S}(\mathcal{H}) \to [0,1]$ をエフェクトとする．任意の状態 $s \in \mathcal{S}(\mathcal{H})$ に対して，$e(s) = \mathrm{tr}\,[sE]$ を満たす，自己共役作用素 E が存在する．さらに，この E は $0 \le E \le \mathbf{1}$ を満たす．アフィン汎関数 e と自己共役作用素 E を同一視して，$0 \le E \le \mathbf{1}$ なる自己共役作用素 E をエフェクトと呼ぶこともある．物理量 M に対応するエフェクト M_i も同様に自己共役作用素と同一視できる．標準単体の定義である確率の規格化条件 $\sum_{i=0}^{n-1} \mathsf{M}_i(s) = 1$ から，作用素として $\sum_{i=0}^{n-1} \mathsf{M}_i = \mathbf{1}$ である．このような，正作用素の組 M_i を (離散) 正作用素値測度 (POVM) といい，M_i のことを POVM 要素という．さらに，任意の i に対して M_i がエフェクト空間の端点 (命題) である射影作用素であるとき，射影作用素の組 M_i を射影作用素値測度 (PVM) という．PVM はスペクトル定理を介して自己共役作用素と対応している．

1.7 縮約状態

合成系の状態 $s \in S_1 \otimes S_2$ に対して，片方の系で物理量の測定を行なうということを考える．この測定を表す物理量を $\mathsf{M}\colon S_1 \to S_{\mathrm{cl}}$，状態空間 S_2 に対応する単位エフェクトを u_2 とすると，$\mathsf{M} \otimes u_2\colon S_1 \otimes S_2 \to S_{\mathrm{cl}}$ が合成系の状態に対する 1 つめの系に対する測定操作を表す．このとき，部分トレース $\mathrm{tr}_2\colon S_1 \otimes S_2 \to S_1$ を次のように定義する．

$$\mathsf{M}(\mathrm{tr}_2\,[s]) = \mathsf{M} \otimes u_2(s). \tag{12}$$

同様にして，$\mathrm{tr}_1\colon S_1 \otimes S_2 \to S_2$ も定義できる．部分トレースもまたアフィン写像であり，状態に対する可能な操作である．この操作を縮約といい，縮約された状態を縮約状態という．この部分トレースは合成系において片方の系のみを扱いたい場合に便利であり，次の章で両立不可能性を定義する際に用いる．古典論の場合はこのトレースを取る操作は同時確率分布から周辺分布を計算する操作に対応している．

2 操作の両立不可能性

上でみたように，量子論には物理量の測定と量子状態から量子状態への状態変化という二種類の操作がある．これらの操作の組は古典論では同時に行なうことが出来るが，量子論では必ずしも同時に行なうことが出来ない．このことを量子論における操作の両立不可能性という．この章では，操作と両立不可能性の定義を行ない，幾つかの具体例を述べる．

2.1 両立不可能性の定義

定義 2.1 (両立可能・不可能). $S_{\mathrm{in}}, S_1, S_2$ を状態空間，$f_1 : S_{\mathrm{in}} \to S_1$，$f_2 : S_{\mathrm{in}} \to S_2$ を操作とする．このとき，$f_1 = \mathrm{tr}_2 \circ f_{12}$，$f_2 = \mathrm{tr}_1 \circ f_{12}$ を満たす操作 $f_{12} : S_{\mathrm{in}} \to S_1 \otimes S_2$ が存在するならば，操作 f_1 と f_2 は両立可能であるという．このような操作が存在しないとき，f_1 と f_2 は両立不可能であるという．

この定義において，それぞれの系が量子，すなわち $S_1 = \mathcal{S}(\mathcal{H}_1)$，$S_2 = \mathcal{S}(\mathcal{H}_2)$ のときについては，合成系は $\mathcal{S}(\mathcal{H}_1) \otimes \mathcal{S}(\mathcal{H}_2) = \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ であることに注意する．これを図で表すと，次の図 1 のようになる．また，両立可能である場合でもこのような性質を満たす f_{12}

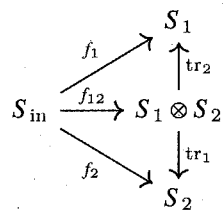

図 1　上の図式が可換であるような f_{12} が存在するとき f_1 と f_2 は両立可能であるという．

は一意とは限らない．両立可能であるということは，操作論的にはそれらの操作を同時に行なうような操作 f_{12} が存在することを意味している．

まず，両立可能な操作の例として縮約を考える．

f_{12} として，恒等写像 id を選べば，図 2 は可換になるので，それぞれの系に対する縮約操作 tr_2 と tr_1 とは両立可能である．このことは，合成系の状態を準備した上で，それぞれの系でそれぞれ実験を行なうということが同時にできるということを意味している．

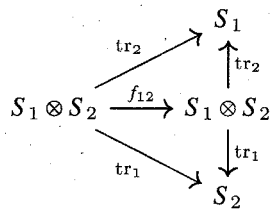

図2　それぞれの系に対する縮約 tr_2 と tr_1 は両立可能である.

2.2　複製禁止定理と配送禁止定理

状態を複製や配送することを考えたい. ここでは, 入出力の状態空間は同じ $S_{\mathrm{in}} = S_1 = S_2 = S$ であるとする. 最初に, 複製という操作を定義する.

定義 2.2 (複製). 操作 $f_C\colon S \to S \otimes S$ と状態 $s \in S$ について,

$$f_C(s) = s \otimes s \tag{13}$$

が成り立つとき, f_C は状態 s の複製 (cloning) であるという.

状態空間の任意の状態を複製するような操作は, 状態空間 S が一点集合である場合を除いて存在しない. このことを背理法で証明する. 状態空間の任意の状態を複製する操作 f_C が存在したとする. 状態空間には $0 < p < 1$ なる実数 p を用いた混合状態 $s = ps_1 + (1-p)s_2$ が存在する. この混合状態を複製すると,

$$\begin{aligned} f_C(s) &= s \otimes s \\ &= (ps_1 + (1-p)s_2) \otimes (ps_1 + (1-p)s_2) \\ &= p^2 s_1 \otimes s_1 + p(1-p)s_1 \otimes s_2 + p(1-p)s_2 \otimes s_1 + (1-p)^2 s_2 \otimes s_2 \end{aligned} \tag{14}$$

であると同時に操作のアフィン性を用いれば,

$$f_C(s) = pf_C(s_1) + (1-p)f_C(s_2) = ps_1 \otimes s_1 + (1-p)s_2 \otimes s_2 \tag{15}$$

である. この式 (14) と (15) の右辺が異なるので, 矛盾している. したがって, 任意の状態を複製するような操作は存在しない.

先の証明の方法からも分かるように, 任意の理論において普遍的な複製操作が存在しないのは混合状態の複製を考えたからである. したがって, 複製を純粋状態に限定してやると複製が存在する可能性はある. 実際に, 古典論においては任意の純粋状態を複製する操作が存在する. 一方で量子論においては任意の純粋状態を複製することが出来ないことが示されて

おり，複製禁止定理として知られている [6, 7]．さらに，任意の純粋状態が複製可能である理論は古典論に限られることが示されている [8]．

複製を古典論において混合状態についても成り立つように拡張したものが配送である．

定義 2.3 (配送)．操作 $f_B\colon S \to S \otimes S$ と状態 $s \in S$ について，

$$\mathrm{tr}_2 \circ f_B(s) = s, \mathrm{tr}_1 \circ f_B(s) = s \tag{16}$$

が成り立つとき，f_B は状態 s の配送 (broadcasting) であるという．

$s = \mathrm{tr}_2[s \otimes s] = \mathrm{tr}_1[s \otimes s]$ より複製は配送であるが，逆は成り立たない．

古典論においては任意の状態を配送する操作が存在することをみる．第 i 成分が 1 で，その他の成分が 0 のベクトルを $\hat{e}_i$ とする．$\sum_{i=0}^{n-1} p_i = 1$ なる正の実数列 p_i を用いて，古典状態は $s = \sum_{i=0}^{n-1} p_i \hat{e}_i$ と表わせる．$f(s) = \sum_{i=0}^{n-1} p_i \hat{e}_i \otimes \hat{e}_i$ と定義すれば，この写像はアフィンであり，任意の状態の配送となっている．したがって，古典論において全ての状態を配送する操作は存在する．

一方で，量子論において任意の状態を配送する操作は存在しないことが示されている [9]．これを，量子論における配送禁止定理という．さらに，任意の状態を配送することが可能な理論は古典論に限られる [8]．両立不可能性の言葉を用いると，恒等操作 $\mathrm{id}\colon S \to S$ と $\mathrm{id}\colon S \to S$ が両立可能であることと，状態空間 S が古典論の状態空間であることが同値である．このように，配送禁止定理は両立不可能性の重要な例となっている．また，配送禁止であることは量子暗号において盗聴者が状態を配送するという戦術で盗聴することが不可能であるということを示しており，応用においても重要な性質である．

2.3 物理量の同時測定可能性

物理量の測定と物理量の測定の両立不可能性について考える．一般論でわかっていることは，任意の物理量の測定が両立可能であることと状態空間が古典であることが同値であるということである [10]．古典論ではない量子論においては両立不可能な測定が存在していることが示唆されている．量子測定理論において，物理量 POVM の両立不可能性は古くから議論されている問題であり，測定の両立不可能性は同時測定可能性 (joint measurability) と呼ばれることもある．よく知られた例として，位置と運動量のように非可換な自己共役作用素で記述される物理量の測定の組は両立不可能である．しばしば，非可換性と両立不可能性は同値であるかのように扱われている．これは自己共役作用素で記述される物理量 (PVM) の場合は正しいが，一般の測定においては同値ではない．

量子論の両立不可能性については，可換な物理量は両立可能である．物理量 A と B が可換であるとは，POVM 要素 A_i と B_j について，

$$\mathsf{A}_i\mathsf{B}_j = \mathsf{B}_j\mathsf{A}_i \tag{17}$$

が任意の i,j に対して成り立つことをいう．このとき，$\mathsf{C}_{ij}=\mathsf{A}_i\mathsf{B}_j$ と定義すれば，C_{ij} は正作用素であり，C は物理量である．この物理量 C を用いれば，物理量 A と B が両立可能であることが示せる．物理量 A と B が可換でない場合は C_{ij} が正作用素になるとは限らないが，あとで述べるような両立可能である例がある．したがって，可換ならば両立可能だが，逆は成り立たない．

PVM，すなわち POVM 要素が射影作用素の場合は，両立可能ならば可換である．正確には，物理量 A と B が両立可能で，少なくとも片方の物理量が PVM ならば，それらの物理量は可換である．このことを証明する．まず，A が PVM であるとしても一般性を失わない．A と B の同時測定を表す物理量を C とする．すなわち，$\sum_j \mathsf{C}_{ij}=\mathsf{A}_i$ と $\sum_i \mathsf{C}_{ij}=\mathsf{B}_j$ を満たす．ここで，$0\le C_{ij}\le \sum_j C_{ij}=\mathsf{A}_i$ が成り立ち右辺が射影作用素なので，

$$\mathsf{C}_{ij}\mathsf{A}_i=\mathsf{A}_i\mathsf{C}_{ij}=\mathsf{C}_{ij} \tag{18}$$

である．$k\neq i$ として，両辺に A_k をかけることで，

$$\mathsf{A}_k\mathsf{C}_{ij}=\mathsf{A}_k\mathsf{C}_{ij}=0 \tag{19}$$

が示せる．

$$\mathsf{A}_k\mathsf{B}_j=\mathsf{A}_k\sum_i \mathsf{C}_{ij}=\mathsf{C}_{kj} \tag{20}$$

かつ

$$\mathsf{B}_j\mathsf{A}_k=\sum_i \mathsf{C}_{ij}\mathsf{A}_k=\mathsf{C}_{kj} \tag{21}$$

なので，A と B は可換である．

PVM ではない一般の POVM に関して，どういった物理量の組が両立可能かという問題は明らかではない．問題を簡単にするため，測定出力が 2 種類の場合を考えたい．すなわち，$\mathsf{A}_0,\mathsf{A}_1=\mathbf{1}-\mathsf{A}_0$，$\mathsf{B}_0,\mathsf{B}_1=\mathbf{1}-\mathsf{B}_0$ のように 2 つの POVM 要素で記述される量子測定を考える．これらの物理量 A と B の測定はそれぞれ 1 つのエフェクト A_0 と B_0 によって特徴づけられている．これらの物理量 A と B が両立可能であるとは

$$\mathsf{C}_{00}+\mathsf{C}_{01}=\mathsf{A}_0,\ \mathsf{C}_{10}+\mathsf{C}_{11}=\mathsf{A}_1,\ \mathsf{C}_{00}+\mathsf{C}_{10}=\mathsf{B}_0,\ \mathsf{C}_{10}+\mathsf{C}_{11}=\mathsf{B}_1 \tag{22}$$

物理量 C が存在するということである．すなわち，

$$\mathsf{C}_{00}=\mathsf{A}_0-\mathsf{C}_{01}=\mathsf{B}_0-\mathsf{C}_{10}=\mathsf{A}_0+\mathsf{B}_0+\mathsf{C}_{11}-\mathbf{1} \tag{23}$$

なるエフェクト C_{ij} が存在すればよい．

最も単純な量子系である量子ビット系について考える．量子ビット系における状態 ρ は，$x^2+y^2+z^2\le 1$ を満たす実数 x,y,z を用いて，

$$\rho=\frac{1}{2}(\mathbf{1}+x\sigma_x+y\sigma_y+z\sigma_z) \tag{24}$$

と書ける．量子ビット系のエフェクト E は，$\|\vec{e}\| \leq e_0 \leq 1 - \|\vec{e}\|$ を満たす実数 e_0, e_1, e_2, e_3 を用いて，

$$E = e_0\mathbf{1} + e_1\sigma_x + e_2\sigma_y + e_3\sigma_z = e_0\mathbf{1} + \vec{e}\cdot\vec{\sigma} \tag{25}$$

とかける．物理量 $\mathsf{A}_0 = a_0\mathbf{1} + \vec{a}\cdot\vec{\sigma}$ と $\mathsf{B}_0 = b_0\mathbf{1} + \vec{b}\cdot\vec{\sigma}$ が両立可能となる条件を考える．$a_0 = b_0 = 1/2$ の場合は，

$$\left\|\vec{a}+\vec{b}\right\| + \left\|\vec{a}-\vec{b}\right\| \leq 1 \tag{26}$$

が成り立つこととAとBが両立可能であることが同値である [11]．

ここまでは，2つの物理量が両立可能である場合を考えてきたが，3つ以上の場合も同様にして定義することは可能である．しかし，3つ以上の場合は難しい．例えば，3つの物理量A，B，Cを考えて，AとB，BとC，CとAのどの二組も両立可能であるとする．このとき，AとBとCが両立可能とならない場合もあるため [12]，問題を2つの物理量の両立不可能性の議論に帰着することが出来ない．もちろん，物理量の測定に限らず，任意の操作について3つ以上の操作の組に関する両立不可能性を議論することは可能であるが，非常に難しいためその性質はあまり調べられていない．

2.4 情報擾乱定理

物理量の測定と状態変化という異なる操作についても両立不可能性について議論ができる．物理量の測定と状態変化が両立可能であるということは，それぞれを実現するインストゥルメントが存在することと同値である．インストゥルメントとは，測定と状態変化を同時に表現するものである．$\mathcal{I}_i : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ は線型なCP写像の組で，$\sum_i \mathrm{tr}\left[\mathcal{I}_i(\rho)\right] = 1$ を満たすものである．この $\mathrm{tr}\left[\mathcal{I}_i(\rho)\right]$ が状態 ρ を準備したときに i が出る確率を表している．$\mathcal{I}_i$ に対応するHeisenberg描像[4]の写像 $\mathcal{I}_i^*$ を用いれば，$\mathrm{tr}\left[\mathcal{I}_i(\rho)\mathbf{1}\right] = \mathrm{tr}\left[\rho\mathcal{I}_i^*(\mathbf{1})\right]$ が確率となるため，$\mathcal{I}_i^*(\mathbf{1})$ が物理量を表しており，実際にCP性と規格化条件からPOVMになっていることが示せる．さらに，チャンネルは $\sum_i \mathcal{I}_i(\rho)$ である．これはTPCP線型写像である．

$$\mathcal{I}_i^*(\mathbf{1}) = \mathsf{A}_i, \ \sum_i \mathcal{I}_i(\rho) = \Lambda(\rho) \tag{27}$$

を満たすインストゥルメント $\mathcal{I}$ が存在するならば，物理量の測定Aと状態変化 Λ が両立可能である．

物理量の測定を行なって情報を得ると，状態が変化してしまう．より多くの情報を得ると，この状態変化は大きくなるという関係を情報と擾乱のトレードオフ関係，あるいは情報

[4] 物理系における変化を状態が変化するものとして考える方法をSchrödinger描像という．一方，物理量の変化として表したものをHeisenberg描像という．Λ のHeisenberg描像の物理量の変化 $\Lambda^* : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ は $\mathrm{tr}\left[\rho\Lambda^*(X)\right] = \mathrm{tr}\left[\Lambda(\rho)X\right]$ で定義される．

擾乱定理という．情報擾乱定理は様々な方法で証明されている [13–19]．多くの情報擾乱定理が情報や擾乱を定量化し，その間に成り立つ不等式を導出することでトレードオフ関係を示している．情報や擾乱を定量化する方法は無数に存在するので，どの定理が良いかは考えている問題や実験の状況による．この情報と擾乱のトレードオフ関係を暗号通信に応用したものが，量子暗号である．定量的な情報と擾乱の関係を用いて，擾乱から漏れた情報量を評価することで，盗聴されたかどうかを判定するのである．

2.5 定性的な情報擾乱定理

定量的な評価は，定量化の方法に依存してしまうという側面がある．様々な情報と擾乱のトレードオフを表す不等式は，情報や擾乱の様々な側面を表している．情報や擾乱は定量化の際に一次元的な値にしてしまうので，情報や擾乱が本来持っていた構造が失われてしまう．そこで，情報と擾乱の関係を定性的な観点から理解し構造を調べようという研究がある [20]．

この研究では事後処理という手法を用いて，情報や擾乱を評価している．一方で，定性的な関係の導入の仕方も一意ではない [21]．そこで，[21] で扱われている定性的な関係である事後処理，状態識別能力，状態決定能力の中で，状態識別能力に着目し，それに対応する擾乱の定性的な関係を発見した [2]．

この後の章では，状態識別能力と擾乱の関係について，それぞれの定義から述べていく．

3 物理量による状態識別能力

この章では，物理量の測定による状態識別可能性を用いて状態識別能力 [21, 22] という関係を物理量の集合に導入する．

物理量 A の測定によって状態 ρ_1 と状態 ρ_2 が識別可能であるとは，$\mathrm{tr}\left[\rho_1 \mathsf{A}_x\right] \neq \mathrm{tr}\left[\rho_2 \mathsf{A}_x\right]$ を満たすような測定出力 $x \in \Omega$ が存在することと定義される．すなわち，何かしらの出力が起こる確率が異なれば，測定結果から入力した 2 状態は異なることが分かるので，状態を識別することができるのである．この識別可能性を用いて，状態識別能力と呼ばれる物理量間の関係を次のように定義する．

定義 3.1. 物理量 B で識別可能な状態の組は物理量 A によっても識別可能であるとき，物理量 A の状態識別能力が物理量 B の状態識別能力よりも高いという．このとき，$\mathsf{A} \gtrsim_i \mathsf{B}$ とかくことにする．

この関係は前順序関係である．すなわち，この関係は反射的 (任意の物理量 A について $\mathsf{A} \lesssim_i \mathsf{A}$ が成り立つ) で推移的 ($\mathsf{A} \lesssim_i \mathsf{B}$ かつ $\mathsf{B} \lesssim_i \mathsf{C}$ ならば $\mathsf{A} \lesssim_i \mathsf{C}$ が成り立つ) である．この

関係は半対称律を満たさないので半順序関係ではない.

全順序関係ではないので, 関係が定義されない物理量の組もある. 例えば, パウリ行列 $\sigma_x, \sigma_y, \sigma_z$ はどちらがより状態識別能力が高いかは, 関係が定義されないので, 比較できないのである.

この, 状態識別能力は POVM の線型包の包含関係と同値である. のちにこの線形空間の次元を用いて定量化する.

もっとも状態識別能力が高い物理量の測定を情報完全な物理量 (informationally complete observables) という. この物理量の測定結果から任意の状態を識別し, 特定することが出来る. 例えば, 量子ビット系でいうと x, y, z 全方向の測定を適当な確率で行なうという測定は情報完全である. 情報完全な物理量の線型包は, 有界線型作用素全体の集合 $\mathcal{B}(\mathcal{H})$ と一致する.

逆に, もっとも状態識別能力が低い物理量の測定はどんなものだろうか. それは任意の状態に対して, 同じ確率分布を返すような測定である. 確率分布が入力状態に依存しないので, 任意の状態の組が識別できない. こういった物理量のことを自明な物理量という. 具体的には, $\mathsf{A}_i = p_i 1$ のように POVM 要素が恒等作用素の定数倍になっている物理量である.

具体例からも分かるように, 最も状態識別能力が高い物理量も, 最も状態識別能力が低い物理量も一意ではない.

4 チャンネルによる擾乱

先の章で状態識別能力を用いて物理量の集合に前順序関係という関係を定義した. この章では, 似たように, チャンネルの集合に前順序関係を入れることを考える. 情報と擾乱の関係を踏まえると, 擾乱に基づいた関係を入れるのが良いだろう.

チャンネル Λ によって状態 ρ が状態 $\Lambda(\rho)$ に変化したあとも, 物理量 B の測定結果は変化していないという場合を考える. ここでは, 状態 ρ と状態 $\Lambda(\rho)$ の両方について, 同じ物理量 B の測定が定義されないといけないので, 同じ状態空間から状態空間へのチャンネルを考えている. すなわち,

$$\mathrm{tr}\left[\rho \mathsf{B}_y\right] = \mathrm{tr}\left[\Lambda(\rho)\mathsf{B}_y\right] \tag{28}$$

が任意の状態 ρ と測定値 y について成り立つとき, チャンネル Λ が物理量 B に擾乱を与えていないという.

チャンネル Λ を定めると擾乱を与えない物理量が定まる. この擾乱を与えないという無擾乱性を用いてチャンネルの集合に関係を入れる.

定義 4.1. Λ_1 と Λ_2 をチャンネルとする. もし, Λ_1 によって擾乱されない物理量が Λ_2 によっても擾乱されないならば, Λ_2 のほうが Λ_1 よりも擾乱が小さいといい, $\Lambda_1 \lesssim_f \Lambda_2$ と

書く.

この関係は状態識別能力と同様に前順序関係になっている.

この無擾乱性による関係はチャンネルの Heisenberg 描像を用いると理解しやすい. チャンネル Λ の Heisenberg 描像を Λ^* とする. すなわち, チャンネル Λ が擾乱を与えない物理量 B について,

$$\mathrm{tr}\,[\rho \mathsf{B}_y] = \mathrm{tr}\,[\Lambda(\rho)\mathsf{B}_y] = \mathrm{tr}\,[\rho \Lambda^*(\mathsf{B}_y)] \tag{29}$$

が成り立つ. これが, 任意の状態 ρ に対して成り立つので, 先の条件は

$$\mathsf{B}_y = \Lambda^*(\mathsf{B}_y) \tag{30}$$

と同じである. この条件を満たす B_y の包含関係で, 前順序関係を定めている. この集合を,

$$\mathrm{Fix}(\Lambda^*) = \{\, X \in \mathcal{B}(\mathcal{H}) \,\big|\, \Lambda^*(X) = X \,\} \tag{31}$$

と書くことにすると, $\Lambda_1 \precsim_f \Lambda_2$ と, $\mathrm{Fix}(\Lambda_1^*) \subset \mathrm{Fix}(\Lambda_2^*)$ が同値である. つまり, 今回導入したチャンネルの前順序関係は Heisenberg 描像のチャンネルの不動点の集合の包含関係に他ならない.

この意味で最も擾乱の小さいチャンネルは入力と同じ状態を出力する恒等チャンネルである. 明らかに, $\mathrm{Fix}(\mathrm{id}^*) = \mathcal{B}(\mathcal{H})$ である. また, 最も擾乱の大きいチャンネルは, 入力した状態に依存せず特定の状態 ρ_0 を返すチャンネルである. Heisenberg 描像におけるこのチャンネルの不動点は恒等作用素 $\mathbf{1}$ の定数倍のみである.

5 情報擾乱の関係

物理量の集合とチャンネルの集合, それぞれに関係を導入した. この章ではこれらの関係を用いて, 物理量とチャンネルが両立可能である場合に物理量やチャンネルにどのような制約がかかるのか考える.

まず, 最初に状態識別能力が最も高い物理量の測定と両立可能なチャンネルについて, 次の性質がなりたつ.

定理 5.1. Λ_{A} を物理量 A と両立可能なチャンネルとする. 物理量 A が情報完全ならば,

$$\mathrm{Fix}(\Lambda_{\mathsf{A}}^*) = \mathbb{C}\mathbf{1}$$

が成り立つ. すなわち, $\Lambda_{\mathsf{A}}^*(B) = B$ を満たす B は $\mathbf{1}$ の定数倍に限られる.

この定理は最も状態識別能力が高い物理量の測定と両立可能なチャンネルは最も擾乱が大きくなるということを主張している.

物理量 A と両立可能なチャンネルの中で最も擾乱が小さいチャンネルを考えたい．一般には最も擾乱が小さいチャンネルというのは定まらないが，次の条件を加えれば，最も擾乱が小さいチャンネルを定めることが出来る．チャンネル Λ をフルランクな不変状態を持つとする．すなわち，$\Lambda(\rho)=\rho$ を満たすフルランク行列 ρ が存在するとする．この条件を満たすチャンネルの中で最も擾乱が小さいチャンネルは定まる．次のように定義される Lüders チャンネル

$$\Lambda_{\mathsf{A}}^{L}(\rho)=\sum_{x}\sqrt{\mathsf{A}_x}\rho\sqrt{\mathsf{A}_x}. \tag{32}$$

は擾乱が最も小さい物理量の測定の 1 つである．

物理量の測定とそれと両立可能なある意味で最も擾乱が小さいチャンネルの間に次の関係が成り立つ．

定理 5.2. Λ_{A}^{L} と Λ_{B}^{L} をそれぞれ物理量 A，B に対応する Lüders チャンネルであるとする．$\mathsf{A}\gtrsim_i \mathsf{B}$ ならば $\Lambda_{\mathsf{A}}^{L}\lesssim_f \Lambda_{\mathsf{B}}^{L}$ が成り立つ．

この定理はより状態識別能力の高い物理量の測定と両立可能なチャンネルは擾乱が大きくなることを表している．

最後に，状態識別能力と無擾乱性を定量化することを考える．状態識別能力と無擾乱性はそれぞれ対応するベクトル空間の包含関係と同値なので，そのベクトル空間の次元を用いた定量化が考えられる．

定理 5.3. 物理量 A とチャンネル Λ が両立可能ならば，

$$\dim\mathcal{L}(\mathsf{A})+\dim\mathrm{Fix}(\Lambda^{*})\leq(\dim\mathcal{H})^{2}+1 \tag{33}$$

が成り立つ．ここで $\mathcal{L}(\mathsf{A})$ は物理量 A の線型包である．さらに，等号成立は物理量 A が情報完全またはチャンネル Λ が恒等チャンネルであることと同値である．

定量化をしてしまうと，もともと定性的な関係が持っていた情報を失うことになる．たとえば，物理量の線型包の次元が同じだからといって，同じ状態識別能力を持つとは限らないわけである．しかし，この定理は最初の定理 5.1 を導くので，少なくとも前順序関係の端の情報は失われていないことが示唆されている．

6 おわりに

本講究録では，量子論における操作の両立不可能性と状態識別能力と擾乱の関係 [2] について述べた．どういう操作の組が両立可能かという問に対する答えは，操作を特徴づける方法によっていくつか作ることが出来るだろう．我々の研究は先行研究 [20] が唯一の定性的な情報擾乱定理ではないということを明らかにしたのである．物理量の集合に導入できる前順

序関係はもう1つ知られているものがあり，状態決定能力と呼ばれている [21]．情報と擾乱の関係を踏まえると，状態決定能力に対応するチャンネルの前順序関係はあるのだろうか？という疑問がある．また，定量化の方法を変えることによって，別の定量的な不等式は導出できないかという，定量化の方法に関する問題も残されている．

今回の後半部では物理量の測定とチャンネルの両立不可能性について扱った．古典情報は配送出来るので，物理量の測定と物理量の測定に関するトレードオフについては状態識別能力を用いた制限は与えられない．実際，情報完全な物理量の測定と情報完全な物理量の測定が両立可能である場合もある[5]．一方，チャンネルとチャンネルの両立不可能性については無擾乱性の観点からも非自明な制限を示すことが出来るだろう．配送禁止定理から，最も擾乱が小さいチャンネルである恒等チャンネルと恒等チャンネルが両立不可能だからである．$\Lambda_1 \colon \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ と $\Lambda_2 \colon \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ を両立可能なチャンネルの組とすると，

$$\dim \mathrm{Fix}(\Lambda_1^*) + \dim \mathrm{Fix}(\Lambda_2^*) \tag{34}$$

について，非自明な制限がある．なぜならば，それぞれの項の最大値は $(\dim \mathcal{H})^2$ であるが，それを単純に足した $2 \times (\dim \mathcal{H})^2$ にならないということが配送禁止定理の主張だからである．しかし，これが実際にどういった値で抑えられるのかは未解決である．

参考文献

[1] T. Heinosaari, T. Miyadera, and M. Ziman, J. Phys. A **49**, 123001 (2016).

[2] I. Hamamura and T. Miyadera, (2016), arXiv:1610.08814 [quant-ph].

[3] J. Barrett, Phys. Rev. A **75**, 032304 (2007).

[4] I. Namioka and R. Phelps, Pac. J. Math. **31**, 469 (1969).

[5] I. Hamamura, 物性研究・電子版 **6**, 062601 (2017).

[6] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[7] D. Dieks, Physics Letters A **92**, 271 (1982).

[8] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, Phys. Rev. Lett. **99**, 240501 (2007).

[9] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[10] M. Plávala, Phys. Rev. A **94**, 042108 (2016).

[11] P. Busch, Phys. Rev. D **33**, 2253 (1986).

[12] T. Heinosaari, D. Reitzner, and P. Stano, Found. Phys. **38**, 1133 (2008).

[13] C. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[5] 同じ物理量は両立可能である．

[14] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).

[15] M. Ozawa, Annals of Physics **311**, 350 (2004).

[16] D. Kretschmann, D. Schlingemann, and R. F. Werner, IEEE Trans. Inf. Theory **54**, 1708 (2008).

[17] F. Buscemi, M. J. W. Hall, M. Ozawa, and M. M. Wilde, Phys. Rev. Lett. **112**, 050401 (2014).

[18] P. Busch, P. Lahti, and R. F. Werner, Phys. Rev. Lett. **111**, 160405 (2013).

[19] T. Shitara, Y. Kuramochi, and M. Ueda, Phys. Rev. A **93**, 032134 (2016).

[20] T. Heinosaari and T. Miyadera, Phys. Rev. A **88**, 042117 (2013).

[21] T. Heinonen, Phys. Lett. A **346**, 77 (2005).

[22] P. Busch and P. J. Lahti, Found. Phys. **19**, 633 (1989).